REMARKS

STATUS OF CLAIMS

Claims 9, 35, 36, and 42 have been amended.

No claims have been added, cancelled, or withdrawn.

Claims 1, 7, 9, 11, 13, 15, 17-18, 27, 29, 31, 33-36, 38-48, 50-60, and 62-72 are currently pending in the application based on the amendments proposed above.

INTRODUCTION

The Applicant proposes to amend Claims 9, 35, 36, and 42 to establish the proper antecedent basis in Claims 9 and 42 for the feature "negative multiplicative inverse of the modulus" as a result of the Examiner's Amendment to the corresponding independent Claims 1 and 36 and to correct typographical errors in Claims 35 and 36 that were inadvertently included in the Examiner's Amendment, as described herein. Because these amendments make the same changes to Claims 9 and 42 as were made in the Examiner's Amendment to other claims and to merely correct typographical errors in Claims 35 and 36, all of whose correction is self-evident from the claims themselves, further substantive reconsideration of Claims 9, 35, 36, and 42 is not required.

AMENDMENTS TO CLAIMS 9 AND 42

Claims 9 and 42 are amended consistent with the Examiner's Amendment to their respective independent Claims 1 and 36, respectively. Specifically, as a result of the Examiner's Amendment accompanying the Notice of Allowance, Claims 1 and 36 now include "a negative multiplicative inverse of the modulus," and therefore Claims 9 and 42 are amended to refer to "the negative multiplicative inverse of the modulus" instead of "~~a~~ negative multiplicative inverse of the modulus."

The changes to Claims 9 and 42 are consistent with the same changes made in the Examiner's Amendment to Claims 11, 13, and 15 that depend on independent Claim 1 and to Claims 39-41 that depend on independent Claim 36.

Also, the change to method Claim 9 parallels the same changes made in the Examiner's Amendment to apparatus Claim 39, computer readable medium Claim 51, and apparatus Claim 63.

Similarly, the change to apparatus Claim 42 parallels the same changes made in the Examiner's Amendment to method Claim 15, computer-readable medium Claim 54, and apparatus Claim 66.

No new matter is added, nor is any further substantive reconsideration of Claims 9 and 42 required.

AMENDMENTS TO CLAIMS 35 AND 36

Claims 35 and 36 are amended to correct a typographical error with the Examiner's amendment. Specifically, at the end of the third to the last step beginning with "generating a first constant...", there are two semi-colons when there should be only one semi-colon. Claims 35 and 36 are amended to delete the extra semi-colon.

The changes to apparatus Claims 35 and 36 make these two apparatus claims consistent with the changes in the Examiner's Amendment to corresponding method Claim 1 and computer-readable medium Claim 34.

No new matter is added, nor is any further substantive reconsideration of Claims 35 and 36 required.

DISCUSSION FOR RULE 312 AMENDMENT

MPEP §714.16 states that amendments that add new claims after allowance must be accompanied by remarks that fully and clearly state the reasons on which reliance is placed to show:

(A) why the amendment is needed;

(B) why the proposed amended or new claims require no additional search;

(C) why the claims are patentable; and

(D) why they were not presented earlier.

Each of these items is addressed below.

(A) WHY THE AMENDMENT IS NEEDED

The amendment is needed to correct four inadvertent errors arising from or in the Examiner's Amendment that accompanied the Notice of Allowance, as described above.

(B) WHY THE PROPOSED AMENDED OR NEW CLAIMS REQUIRE NO ADDITIONAL SEARCH

As amended, Claim 9 recites the same features as in Claims 39, 51, and 63. The amendment to Claim 9 is the same as in Claims 11, 13, and 15 and is made for the same reason, namely to establish the proper antecedent basis for "negative multiplicative inverse of the modulus."

Similarly, Claim 42 recites the same features as in claims 15, 54, and 66. The amendment to Claim 42 is the same as in Claims 39-41 and is made for the same reason, namely to establish the proper antecedent basis for "negative multiplicative inverse of the modulus."

Finally, as amended, Claims 35 and 36 recite the same features as in Claims 1 and 34.

Therefore, no new search is needed since these features of Claims 9, 35, 36, and 42 have been searched as part of the examination of Claims 11, 13, 15, 39-41, 51, 54, 63, and 66.

(C) WHY THE CLAIMS ARE PATENTABLE

The amended claims are patentable for the same reasons given in Applicants' prior correspondence in this prosecution and because the amendments herein relate strictly to minor formal matters that do not substantively change the scope of the claim.

(D) WHY THEY WERE NOT PRESENTED EARLIER

The claims as amended herein were not earlier presented because Applicants first identified these inadvertent errors that arose from the Examiner's Amendment and that are corrected herein upon reviewing the Examiner's Amendment that was received with the Notice of Allowance.

INTERVIEW SUMMARY

The Applicant thanks the Examiner for the Interview conducted on May 12, 2005. The interview was between Examiner Longbit Chai and the applicant's attorney,

Craig G. Holmes. Pending Claims 1, 6, and 34-37 that were rejected in the Office Action mailed on January 6, 2005 were discussed along with U.S. Patent Application Publication No. 2003/0031316 of Langston et al.

Note that the Interview Summary provided by the Examiner with the Notice of Allowance refers to Claim 2, but this reference should be to Claim 6 instead because the features of Claim 6, not Claim 2, are incorporated into Claim 1 via the Examiner's Amendment (along with similar changes to the other independent claims) and because Claim 2 was previously cancelled in the Office Action Response filed on April 6, 2005.

The discussion during the interview focused on potential amendments to Claim 1 and the other independent Claims 34-37. Specifically, the Examiner and the Applicant discussed the incorporation into Claim 1 of the features of Claim 6, along with adding to the preamble the feature of "a modular reduction using a negative multiplicative inverse of the modulus." Agreement was reached that the amendments discussed would place the application in condition for allowance, and the Applicant agreed to send the Examiner a proposed amendment to the claims consistent with the amendments discussed to facilitate the Examiner's entry of an Examiner's Amendment.

CONCLUSION

For the foregoing reasons, entry and allowance of the amendments presented by this amendment is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims remain in condition for allowance.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Craig G. Holmes
Reg. No. 44,770

Date: September 7, 2005

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
Telephone: (408) 414-1207
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, Mail Stop ISSUE FEE, P.O. Box 1450, Alexandria, VA 22313-1450.

on 9/7/05 by Trudy Bigelow